S. AMANDA MARSHALL, OSB #95347
United States Attorney
District of Oregon
ANNEMARIE SGARLATA, OSB #065061
Assistant United States Attorney
annemarie.sgarlata@usdoj.gov
DONNA B. MADDUX, OSB #023757
Assistant United States Attorney
donna.maddux@usdoj.gov
1000 S.W. Third Ave., Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
Facsimile: (503) 727-1117
Attorneys for United States of America

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

UNITED STATES OF AMERICA

v.

RACHEL LEE,

Defendant.

No. 3:14-CR-00184(1)-JO

GOVERNMENT'S RESPONSE TO DEFENDANT RACHEL LEE'S MOTION TO STAY THE EXECUTION OF SEARCH AND SEIZURE WARRANT

The United States of America, by S. Amanda Marshall, United States Attorney for the District of Oregon, and through AnneMarie Sgarlata and Donna Brecker Maddux, Assistant United States Attorneys, hereby submits this response to defendant Rachel Lee's motion to stay the execution of e-mail and cellular telephone search warrants in the above-captioned case.

I. BACKGROUND

On May 7, 2014, defendant, two of her daughters, and her significant other were indicted by a federal grand jury on wire fraud and money laundering conspiracy charges. (CR[1] 1 in U.S. District Court Case No. 14- CR-00184-JO). On June 23, 2014, the government submitted six sealed applications for search warrants for electronic communications and other information stored at internet service or cellular telephone providers (hereinafter "communication service providers"). Each proposed warrant authorized the search of specific subscriber accounts and the seizure of evidence of violations of wire fraud, money laundering and tax statutes from December 1, 2007 to present. Each application included an affidavit providing factual information to support a finding of probable cause, along with attachments specifying the places to be searched and the particular items to be seized. (CR[2] 1, 9, 17, 25, 33, and 41). The affidavits and attachments each set forth substantially the same two-step protocol for searching any information that the communication service providers provided in response to the warrants, and for seizing any information falling within the timeframe and subject matter specified in the warrant applications and attachments.

On June 23, 2014, U.S. Magistrate Judge Paul Papak issued the warrants, finding probable cause to believe that evidence of violations of wire fraud, money laundering, and tax

[1] "CR" stands for the Clerk's Record and the digit that follows it refers to the document number in the Clerk's Record of the applicable case number.

[2] Except where stated otherwise, this reference and all further references to the Clerk's Record herein, refer to the record in U.S. District Court for the District of Oregon case number 14-mc-00252, the miscellaneous case number under which the search warrants were docketed.

statutes could be found in the places to be searched and items to be seized. (CR 2, 10, 18, 26, 34, and 42). On August 12, 2014, investigating agents returned the search warrants executed, certifying that the communication service providers provided the data and information required by the warrants. (CR 61- 65).

On August 15, 2014, before investigating agents began searching the data to seize any items permitted by the warrants, defendant filed a motion to stay the investigating agents' search. (CR 65 in Case No. 14-CR- 00184-JO). Defendant argues that the search warrants aren't sufficiently particular, and that their protocols "taint" the prosecution team by exposing investigative agents to data they are not authorized to seize under the warrants. She urges the Court to halt the search and require the government to foreswear the plain view doctrine as a prophylactic measure to mitigate any "taint" that she says might result from implementation of the established two-step protocol[3]. For the reasons below, this Court should deny defendant's motion.

II. ARGUMENT

A. No authority supports the relief Defendant seeks.

Defendant's motion should be denied because a movant cannot challenge a search warrant, a magistrate judge's finding of probable cause, or a search protocol described in a warrant's affidavit and attachments before a search has taken place. *United States v. Grubbs*, 547 U.S. 90 (2006). Neither the Federal Rules of Criminal Procedure nor the Fourth Amendment entitle a property owner to even a copy of the warrant until after the search has been conducted[4].

[3] Defendant does not now challenge the adequacy of the probable case upon which the warrants were issued.

[4] In this case, Defendants were provided copies of the search warrants, applications, affidavits and attachments before the investigating agents began their review of materials provided by the communication service providers. This was to allow defendants to work with a non-prosecution-team Assistant U.S. Attorney and a non-prosecution-team agent (the "filter team") in reviewing a protocol for the filter team to follow in screening and removing from

Id. Nor does the particularity requirement of the Fourth Amendment provide or protect any interest in monitoring searches conducted pursuant to a warrant. *Id*. at 99.

Defendant cannot rely on Rule 41(g) of the Federal Rules of Criminal Procedure, as that rule provides a mechanism for relief *after* an unlawful search and seizure. *See* Fed. R. Crim. P. 41(g). No rule provides a mechanism for relief *before* the search of an authorized location and seizure of items specified in the warrant has taken place. Defendant cites no authority to the contrary.

While Defendant suggests that *Riley v. California*, 134 S. Ct. 2473 (2014), supports her position, *Grubbs* is the controlling Supreme Court case. The issue before the Court in *Riley* was whether the search-incident-to-arrest exception to the Fourth Amendment's warrant requirement applies to the search of a cell phone incident to its possessor's arrest. *Riley*, 134 S. Ct. at 2484. The issue in *Grubbs* was the issue at bar here: whether the Constitution grants property owners the right to challenge a validly-issued search warrant before the search has taken place. *Grubbs*, 547 U.S. 90. The Supreme Court in *Grubbs* held it does not, and reversed the Ninth Circuit Court of Appeals' decision to the contrary. The Court explained:

> The absence of a constitutional requirement that the warrant be exhibited at the outset of the search, or indeed until the search has ended, is ... evidence that the requirement of particular description does not protect an interest in monitoring searches. The Constitution protects property owners not by giving them license to engage the police in a debate over the basis for the warrant, but by interposing, *ex ante*, the deliberate, impartial judgment of a judicial officer ... between the citizen and the police, and by providing *ex post* a right to suppress evidence improperly obtained and a cause of action for damages.

Id. at 99 (citations and quotations omitted).

The Supreme Court made clear in *Grubbs* that a warrant is not issued to allow property owners the right to monitor the police; the magistrate judge monitors the police by deciding

---

the materials any potentially attorney-client privileged communications before the materials were provided to prosecution team agents to search for and seize materials covered by the search warrants.

whether a warrant should be issued in the first place. An aggrieved party can file a motion to suppress or a motion for return of property afterward.

Riley is not to the contrary. Nothing in that case supports a conclusion that defendant, the subscriber or user of email or cellular telephone accounts[5], is entitled to more protection than the residential property owner in *Grubbs*. Rather, both cases make clear that a neutral and detached magistrate's finding of probable cause "is the quintessential precondition to the valid exercise of executive power," *Grubbs*, 547 U.S. at 98, and is the constitutional protection afforded a property owner before a search or seizure occurs. *See Riley*, 134 S. Ct. at 2482. Otherwise, courts would spend substantial time and resources reviewing un-executed warrants that were validly issued by a neutral and detached judicial officer in the first place. Defendant presents nothing to indicate that Magistrate Judge Papak reviewed the warrant applications with anything less than a deliberate and impartial eye. He is entitled to the presumption that he fulfilled his duty as a judicial officer.

Because defendant is attempting to do exactly what she cannot do - challenge the warrants *ex ante* - she is without standing and her motion should be denied. If denied on these grounds, this Court need not entertain the remainder of defendant's arguments here. Regardless, defendant's arguments that the warrant is overbroad, that the protocol is flawed, and that agents must forswear the plain view doctrine also fail.

B. The warrants are sufficiently particular.

The Fourth Amendment provides that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the

[5] Since the prosecution team cannot begin reviewing the materials until the privilege review conducted by the filter team and the defense attorneys is complete, it isn't even clear which of the e-mail or cellular telephone accounts defendant Rachel Lee has used or operated. Until then, it remains to be seen whether she has even a theoretical privacy interest in any or all of the accounts in question and the standing required to even contest the search or seizure of any particular account.

persons or things to be seized." U.S. Const. amend. IV. "As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is reasonableness." *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995)(internal quotation marks omitted). "Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant." *Id*. at 653.

The warrant must describe with particularity two items: (1) the place to be searched, and (2) the persons or things to be seized. *Grubbs*, 547 U.S. at 97. The Supreme Court has rejected efforts to expand the scope of this provision to embrace any other matters. *Id*. at 97. Notably, "[n]othing in the language of the Constitution or in [the Supreme Court's] decision interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed." *Dalia v. United States*, 441 U.S. 238, 257 (1979).

A search warrant sufficiently describes the place to be searched if the executing officer "can, with reasonable effort ascertain and identify the place intended." *United States v. Vaughn*, 830 F.2d 1185, 1186 (D. C. Cir. 1987)(internal quotation marks and citation omitted). "By limiting the authorization to search to the specific areas and things for which there is probable cause to search," the Supreme Court has explained, "the [particularity] requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

The search warrants in this case are sufficiently particular. Each one limits law enforcement's discretion to determine the location to be searched by identifying the particular e-

mail and cellular telephone accounts agents are permitted to search. Each one constrains law enforcement's discretion by limiting the seizure to information of a particular subject matter: data from December 1, 2007 to present that constitute evidence of violations of 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1956 (Money Laundering); and 26 U.S.C. § 7201 (Tax violations). These limitations are reasonable and sufficient under the circumstances here. *See, e.g.*, *United States v. Needham*, 718 F.3d 1190, 1196 (9th Cir. 2013)(child pornography warrant is not an impermissible "general warrant" where it "specified what law enforcement sought (child pornography or evidence of its receipt and/or distribution), and where it was believed they would find it (in [defendant's] paper documents or electronic media");*United States v. Adjani*, 452 F.3d 1140, 1147–48 (9th Cir.2006) ("Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible") (citation omitted); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997)(holding valid a warrant authorizing the "blanket seizure" of defendant's "entire computer system" because the government did not know where at least two illicit child pornography images were stored and "no more specific description of the computer equipment sought was possible").

C. The search warrant protocol is valid.

Following the two-step protocol specified in the warrants does not give rise to a constitutional violation. Rule 41(e) sets forth the requirements for issuing a warrant, including the information that must be contained in the warrant and the proper protocol for executing the warrant. Fed. R. Crim. P. 41(e). It authorizes courts to issue warrants for the "seizure of electronic storage media or the seizure or copying of electronically stored information," and expressly provides for a subsequent off-site review of electronic information in accordance with the warrant. Fed. R. Crim. P. 41(e)(2)(B); *United States v. Schesso*, 730 F.3d 1040, 1046 at n.3

(9th Cir. 2013)("[Rule 41(e)(2)(B)] explicitly permits the seizure or copying of electronically stored information for later off-site review"). The Advisory Committee's Notes to the 2009 amendments of Rule 41(e)(2)(B) explain why:

> Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.

Fed.R.Crim. P. 41(e)(2) adv. comte. note.

The search protocols Defendant decries in this case follow the two-step procedure authorized by the Rule and explained in the notes. Under those procedures, the internet service provider or cellular phone company is required to disclose information pertaining to a specific subscriber account. (CR 41 at 15-17 and 25-27)[6]. Upon receiving the relevant records, the government is to search the information obtained and seize what falls within the parameters of the warrants. *Id*.

This process comports not just with Rule 41, but also with the Constitution. Courts regularly find similar or identical procedures to be reasonable under the Fourth Amendment, where there is a valid warrant supported by probable cause. *See Schesso*, 730 F.3d at 1046 (upholding government's seizure of electronic data for a subsequent off-site search where there was a fair probability that evidence would be found on the defendant's personal computer and other electronic devices); *United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012)("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit

[6] Each search and seizure warrant contains substantially the same two-step protocol.

demonstrate a 'sufficient chance of finding some needles in the computer haystack.'" (*quoting United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999)). *See also United States v. Haywood*, 464 F.2d 756, 760 (D.C. Cir. 1972)("The Federal Rules of Criminal Procedure are carefully tailored ground rules for fair and orderly procedures in administering criminal justice. Rule 41 embodies standards which conform to the requirement of the Fourth Amendment.").

United States v. Comprehensive Drug Testing, Inc. ("CDT III,"), 621 F.3d 1162 (9th Cir. 2010)(en banc)(per curiam) is not to the contrary. As the Ninth Circuit observed in *Schesso*, the absence of "*CDT II*'s" suggested protocols in the warrant at issue there "neither violates the Fourth Amendment nor is inconsistent with '*CDT III,*'" in light of the fact that the prophylactic search protocol suggested in "*CDT II*" is "no longer binding circuit precedent." *Schesso*, 730 F.3d at 1047, 1049

D. Waiver of the plain view exception is unnecessary.

Waiver of the plain view exception was not required in *Schesso* and it is not required here. "*CDT III*" does not assist Defendant's argument because unlike here, the warrant in that case issued subject to certain procedural safeguards that the government failed to follow. "*CDT III,*" 621 F.3d at 1168-72. It was under those circumstances that the court required the government to waive plain view in that case. *Id*.

In his concurrence in "*CDT III,*" Chief Judge Kozinski encouraged magistrate judges to insist that the government "foreswear reliance on the plain view exception" as to any other incriminating items that come into view when searching data for the items to be seized. *Id.* at 1178. When signing the warrants at issue, Magistrate Judge Papak did not require the government to waive the plain view exception during execution. Magistrate Judge Papak

decision not to impose this additional requirement does not render the warrants in this case invalid or otherwise flawed.

III. CONCLUSION

This Court should deny Defendant's motion because there is no case or controversy; her issue is not ripe and the remedy she seeks is not supported by law. Failing that, her motion should be denied on the merits because the search warrants are not unconstitutionally overbroad, the search protocols are sufficient, and the circumstances here do not warrant a requirement that the government foreswear the plain view doctrine.

DATED this 4th day of September 2014.

Respectfully submitted,

S. AMANDA MARSHALL
United States Attorney

/s/ AnneMarie Sgarlata
ANNEMARIE SGARLATA, OSB #065061
Assistant United States Attorney

/s/ Donna Maddux
DONNA BRECKER MADDUX, OSB #023757
Assistant United States Attorney